Guía de instalación v3.3.0

TPM (Trusted Platform Module)

computers.toshiba-europe.com

TOSHIBA
Leading Innovation

Contenido

1 Introducción 4
1.1 Convenciones 4
1.2 TPM: Descripción general 5

2 Utilización de TPM por primera vez 6
2.1 Activación de TPM 6
2.2 Instalación de Infineon TPM Professional Package 7
2.3 Registro de propietarios y usuarios en TPM 8

3 Personal Secure Drive 13
3.1 Ventajas que ofrece Personal Secure Drive (unidad segura personal) 13
3.2 Personal Secure Drive (PSD): funcionamiento sencillo 13

4 Secure E-Mail 16
4.1 Configuración 16

5 EFS (Encrypting File System) Extension (extensión de EFS -sistema de cifrado de archivos-) 17

6 Utilidad de contraseña de TOSHIBA 19

7 Migración del entorno TPM y eliminación 20
7.1 Migración 20
7.2 Eliminación del PC 21

8 Recuperación de TPM 22
8.1 Emergency Recovery Process (proceso de recuperación de emergencia): Descripción general 22
8.2 Restablecimiento la contraseña de usuario 22
8.3 Restauración de PSD 22

Índice

Copyright

Los derechos de Copyright de este manual pertenecen a Toshiba Corporation con todos los derechos reservados. De acuerdo con las leyes de propiedad intelectual, este manual no puede reproducirse en forma alguna sin el permiso previo y por escrito de Toshiba. Toshiba no se hace responsable de ninguna patente respecto al uso de la información incluida en este manual.

© 2008 Toshiba Corporation. Todos los derechos reservados.

Marcas comerciales

Microsoft, Windows y Windows Vista son marcas registradas de Microsoft Corporation en EE.UU. y/o en otros países.

El resto de marcas y nombres de productos son marcas comerciales o registradas de sus respectivas empresas propietarias.

1 Introducción

Su ordenador cuenta con un módulo de plataforma de confianza integrado (Trusted Platform Module: TPM). Para activar TPM, tendrá que activarlo o instalar el software Infineon Security Platform Tools. En esta guía de instalación se describe cómo instalar y configurar TPM. Antes de utilizar TPM, lea detenidamente la Guía de instalación.

1.1 Convenciones

Esta guía utiliza los siguientes formatos para describir, identificar y resaltar términos o procedimientos operativos.

Iconos de seguridad

Esta guía contiene instrucciones de seguridad que debe tener en cuenta para evitar posibles situaciones peligrosas que pudieran ocasionarle daños personales o en el equipo, así como la pérdida de los datos. Estas precauciones de seguridad se han clasificado según la seriedad del riesgo, al tiempo que los iconos resaltan estas instrucciones del siguiente modo:

Indica una situación de riesgo potencial que, si no se evita, puede provocar daños materiales.

Proporciona información importante.

1.2 TPM: Descripción general

El controlador de seguridad integrado TPM se basa en las especificaciones de Trusted Computing Group. TPM ofrece protección de datos mediante el uso de claves de cifrado secretas en lugar de fórmulas de cifrado secretas (algoritmos). Con el cifrado basado exclusivamente en software, existe el peligro que de la clave de cifrado guardada en el archivo o leída en la memoria del PC pudiera ser leída y descifrada. Al almacenar la clave de cifrado en TPM, los datos cuentan con una mayor protección.

Dado que TPM utiliza especificaciones públicas y estandarizadas, es posible crear un entorno de PC más seguro mediante el uso de la solución de seguridad correspondiente.

Para obtener información adicional sobre la especificación TCG, visite el sitio Web http://www.trustedcomputinggroup.org/

Cifrado, certificados y contraseñas

- *TPM ofrece una función para crear y configurar múltiples claves de cifrado, certificados y contraseñas. Una vez configurados, asegúrese de que las contraseñas se almacenan en lugar seguro y de que se realiza una copia de seguridad de los archivos de clave de cifrado. Si esta configuración se pierde o se olvida, los archivos cifrados mediante este TPM no podrán descifrarse y no será posible acceder a los datos cifrados.*

TPM

- *Aunque TPM ofrece las funciones de seguridad más avanzadas, no garantiza una protección completa de datos y hardware. Toshiba no se hace responsable de fallos o daños que pudieran deberse al uso de esta función.*

Si se han registrado varios usuarios en ® Windows® y estos usuarios van a usar TPM, cada usuario deberá iniciar una sesión en Windows® y registrarse individualmente.

2 Utilización de TPM por primera vez

Este manual contiene sólo las directrices generales. Consulte y lea la ayuda de TPM tras instalar TPM Professional Package.

Al utilizar TPM por primera vez, deberá configurarlo de la siguiente forma. (Los parámetros de configuración 1 - 3 pueden establecerse iniciando una sesión como administrador de *Windows*®.)

1 Active TPM.
2 Instale **Infineon TPM Professional Package**.
3 Registre el propietario y los usuarios en TPM.

2.1 Activación de TPM

Para activar TPM, haga lo siguiente en la configuración de la BIOS:

1 Mantenga pulsada la tecla **Esc** mientras enciende el ordenador.
2 Aparece un mensaje. Pulse la tecla **F1.**
3 Aparecerá la pantalla BIOS Setup (Configuración de la BIOS).
4 Pulse **PgDn** para ver la siguiente pantalla.
5 Establezca **TPM** en **SECURITY CONTROLLER** con el valor **Enabled** (activado).

En algunos modelos, es posible que se incluya **Hide TPM** *(ocultar TMP) como opción en la pantalla de configuración de la BIOS. Si el sistema muestra* **Hide TPM**, *deberá establecer esta opción con el valor* **No** *antes de establecer* **TPM** *con el valor* **Enabled** *(activado). En caso contrario, no podrá cambiar* **TPM**.

6 Pulse la tecla **End**, guarde los cambios en la configuración de la BIOS y pulse la tecla **Y**.

No se garantiza la coherencia interna de datos en TPM si el ordenador se envía a reparar. Antes de enviar el ordenador a reparar, realice una copia de seguridad no sólo de los archivos de la unidad de disco duro, sino también de los datos de TPM utilizando la función de copia de seguridad. (Consulte el Capítulo 8 - Recuperación de TPM*.) Las funciones de seguridad que utilizan TPM no pueden continuar funcionando correctamente si se pierden los datos de TPM. (Ejemplo: Los archivos cifrados con TPM ya no podrán abrirse.) En este caso, podría perder datos.*

- ***TPM** se entrega configurado de manera predeterminada con el valor **Disabled** (desactivado). Asimismo, puede haber casos en los que **TPM** se configure con el valor **Disabled** tras enviar el ordenador a reparar. Active TPM configurándolo de nuevo.*
- *Para evitar que nadie que no sea el administrador y los usuarios de este ordenador pueda cambiar la configuración de la BIOS, se recomienda encarecidamente configurar una contraseña de la BIOS y una contraseña de supervisor de la BIOS. Consulte el Manual del usuario del ordenador para conocer cómo se configuran estas contraseñas.*

2.2 Instalación de Infineon TPM Professional Package

Instale **Infineon TPM Professional Package** mediante `C:\TOSHIBA\Drivers\TPM Utility`.

Infineon TPM Professional Package incluye el siguiente software y funciones:

- Security Platform Help
- Security Platform Settings Tool
- Security Platform Initialization Wizard
- Security Platform User Initialization Wizard
- Security Platform Migration Wizard
- Security Platform Backup Wizard
- Security Platform Password Reset Wizard
- Security Platform PKCS #12 Import Wizard
- Security Platform Certificate viewer and Certificate Selection
- Security Platform Taskbar Notification Icon
- Security Platform Integration Services
  - Microsoft® Outlook® Integration
  - Netscape® Integration
  - Encrypted File System Integration
  - Personal Secure Drive
  - Policy Administration
- Security Platform Services
  - TSS (TCG Software Stack) Service Provider
  - TSS Core Service
  - TSS Device Driver Library

2.3 Registro de propietarios y usuarios en TPM

1 Haga clic en el icono **Security Platform** (plataforma de seguridad) en la barra de tareas y seleccione **Security Platform Initialization** (inicialización de plataforma de seguridad).

2 TPM se inicia y aparece su pantalla. Haga clic en el botón **Next** (siguiente).

3 En la pantalla **Initialization** (inicialización), seleccione Initialize a new Security Platform (inicializar una nueva plataforma de seguridad). Haga clic en el botón **Next** (siguiente).

4 En la pantalla **Create Security Platform Owner** (crear propietario de plataforma de seguridad) para autenticación del propietario, introduzca la contraseña en los cuadros de texto **Password** (contraseña) y **Confirm Password** (confirmar contraseña) y haga clic en el botón **Next** (siguiente).

5 Aparecerá la pantalla **Features** (funciones). Seleccione la función de Security Platform (plataforma de seguridad) que desea establecer y haga clic en el botón **Next**. Consulte la ayuda para más detalles sobre las funciones de Security Platform.

Se recomienda configurar **Automatic Backup** *(copia de seguridad automática). Si no se configura, los datos de usuario cifrados podrían perderse si surgen problemas.*

6 En la pantalla **Backup** (copia de seguridad), especifique la ubicación en la que debe crearse y guardarse el archivo de copia de seguridad. Haga clic en el botón **Next** (siguiente).

7 En la pantalla **Emergency Recovery** (recuperación de emergencia), seleccione **Create a new Recovery Token** (crear nueva ficha de recuperación) y especifique la ubicación en la que debe crearse y guardarse la **Emergency Recovery Token** (ficha de recuperación de emergencia).

8 En la pantalla **Emergency Recovery** (recuperación de emergencia) para autenticación de **Emergency Recovery Token** (ficha de recuperación de emergencia), introduzca la contraseña en los cuadros de texto Password (contraseña) y Confirm Password (confirmar contraseña) y haga clic en el botón **Next** (siguiente).

Se recomienda encarecidamente la creación de una ficha de recuperación de emergencia de manera que la información de TPM y los datos de usuario relacionados con TPM estén seguros en el caso de que se produzca un problema grave en el sistema. El no seguir esta recomendación puede provocar posibles pérdidas de datos.

9 En la pantalla **Password Reset** (restablecimiento de contraseña), seleccione **Create a new Token** (crear nueva ficha) y especifique la ubicación en la que debe crearse y guardarse la **Password Reset Token** (ficha de restablecimiento de contraseña).

10 En la pantalla **Password Reset** (restablecimiento de contraseña) para autenticación de **Password Reset Token** (ficha de restablecimiento de contraseña), introduzca la contraseña en los cuadros de texto Password (contraseña) y Confirm Password (confirmar contraseña) y haga clic en el botón **Next** (siguiente).

Se recomienda encarecidamente crear y guardar la **Password Reset Token** *(ficha de restablecimiento de contraseña) en un soporte de almacenamiento, como un disquete, de manera que esté accesible aun en el caso de que se produzca un fallo en el ordenador. Asegúrese de que guarda el disco en un lugar seguro por si necesita utilizarlo en el futuro.*

- Si hay varios ordenadores con TPM, la ficha de cada ordenador es diferente y debe almacenarse por separado.
- No es posible volver a crear la ficha de recuperación para el propietario de TPM registrado*. Para evitar pérdidas, deberán crearse y almacenarse varias copias de la ficha tal y como se ha recomendado anteriormente.

  *Puede crearse el mismo nombre de propietario de TPM inicializando TPM en el menú de la BIOS y registrando un nuevo propietario. No obstante, dado que el propietario es en realidad diferente al propietario anteriormente registrado en este caso, los archivos cifrados previamente no podrán descifrarse.
- Si la ficha se filtra o resulta robada por terceros junto con la contraseña, podrán acceder a los datos cifrados. Por consiguiente, se recomienda almacenar las fichas y las contraseñas de forma cuidadosa.

  Consulte el Capítulo 8 - *Recuperación de TPM*.

11 Aparecerá el **Summary** (resumen). Seleccione el resumen y haga clic en el botón **Siguiente**.

12 Puede que el mensaje **Wizard completed successfully** (el asistente ha finalizado correctamente) tarde en aparecer varios minutos. A continuación, haga clic en la casilla de verificación **Start Security Platform User Initialization Wizard** (iniciar asistente de inicialización de usuario de plataforma de seguridad) y luego haga clic en el botón **Finish** (finalizar).

13 En la pantalla **User Initialization Wizard** (asistente de inicialización de usuario), haga clic en el botón **Next** (siguiente).

14 En la pantalla **Basic User Key Password** (contraseña de clave básica de usuario) para autenticación del usuario, introduzca la contraseña en los cuadros de texto **Password** (contraseña) y **Confirm Password** (confirmar contraseña) y haga clic en el botón **Next** (siguiente).

15 En la pantalla **Basic User Password Reset** (restablecimiento de contraseña de usuario básico), asegúrese de que está seleccionada la opción **Enable the resetting of my Basic User Password in case of an emergency** (permitir el restablecimiento de mi contraseña de usuario básico en caso de emergencia). Especifique la ubicación para crear y guardar el archivo **Personal Secret** (secreto personal).

Guarde este archivo en un lugar seguro. En caso de necesidad, tendrá que utilizarlo para restablecer la contraseña de usuario básico.

16 Aparecerá la pantalla **Password and Authentication** (contraseña y autenticación). Confirme el contenido mostrado y haga clic en el botón **Next**.

Puede que la pantalla Security Platform Features (funciones de la plataforma de seguridad) tarde varios minutos en aparecer.

17 Asegúrese de que están seleccionadas las funciones deseadas en la pantalla **Security Platform Features** (funciones de plataforma de seguridad) y haga clic en el botón **Next**.

- *Para utilizar* **Secure E-mail** *(correo electrónico seguro), es preciso establecer la configuración en* **Mail Software** *(software de correo). Consulte el Capítulo 4 -* Secure E-Mail *para obtener información sobre el correo electrónico seguro.*
- *La función* **File and Folder encryption (EFS)** *(cifrado de archivos y carpetas) no está disponible en Windows Vista® Home.*
- *Es preciso formatear la unidad de disco duro con el formato NTFS para utilizar la función* **File and Folder encryption (EFS)***.*

Las opciones establecidas en esta sección también pueden modificarse con posterioridad a la configuración.

18 Si se selecciona **Secure E-mail** (correo electrónico seguro) en la pantalla **Security Platform Features** (funciones de plataforma de seguridad), aparecerá la siguiente pantalla. Haga clic en el botón **Next** (siguiente).

Si se hace clic en alguno de los botones de **Outlook®**, **Windows Mail/ Outlook Express** *o* **Netscape®** *de la pantalla, aparecerá la ayuda para la configuración de* **Secure E-mail** *con el correspondiente software de correo,* **Mail Software***. (Es posible ver esta ayuda incluso después de que finalice el asistente.)*

19 El mensaje de emisión de **Encryption Certificate** (certificado de cifrado) aparece en la pantalla Security Platform Features (funciones de la plataforma de seguridad). Seleccione el certificado que debe emitirse y haga clic en el botón **Next**. Normalmente, deberá hacer clic en el botón **Create** (crear) para crear y seleccionar el certificado.

El valor predeterminado de **Maximum Basic User Password age** *(duración máxima de la contraseña de usuario básico) esta configurada con el valor* **[Disabled]** *(desactivada). Especifique la duración máxima de la contraseña de usuario básico en* **User** *(usuario), en* **Security Policy** *(directiva de seguridad).*

20 Si se selecciona **Personal Secure Drive (PSD)** (unidad segura personal) en la pantalla **Security Platform Features** (funciones de plataforma de seguridad), aparecerá la siguiente pantalla. En esta pantalla, seleccione la unidad que desea asignar a PSD, luego introduzca el nombre de la etiqueta de la unidad y haga clic en el botón **Next**. Consulte el Capítulo 3 - *Personal Secure Drive* para obtener información sobre Personal Secure Drive (PSD).

21 En la pantalla **Security Platform Features** (funciones de plataforma de seguridad), introduzca el volumen del espacio de almacenamiento que desea asignar a PSD, luego seleccione la unidad y haga clic en el botón **Next**.

22 Aparecerá Confirm setting (confirmar configuración), tras lo cual deberá hacer clic en el botón **Next**.

- *Se recomienda encarecidamente especificar una unidad de disco duro integrada (normalmente la unidad C) en el menú desplegable* **My Personal Secure Drive will be saved on this drive** *(mi unidad segura personal se guardará en esta unidad).*
- *El espacio disponible en la unidad especificada más arriba debe ser superior al espacio especificado en* **My Personal Secure Drive will have [XX] MB of storage space** *(mi unidad segura personal tendrá XX MB de espacio de almacenamiento).*

23 Después de unos instantes, aparecerá el mensaje **Wizard completed** (asistente finalizado). Haga clic en **Finish** (finalizar).

Si se han registrado varios usuarios en Windows® y estos usuarios van a usar TPM, cada usuario deberá iniciar una sesión en Windows® y registrarse individualmente. Tras iniciar una sesión en Windows® para realizar el registro de usuario, haga clic en el icono **Security Platform** *(plataforma segura) en la bandeja de tareas y seleccione* **Security Platform User initialization** *(inicialización de usuario de plataforma de seguridad).*

Al modificar la configuración, haga clic en el icono **Security Platform Setting Tool** (herramienta de configuración de plataforma de seguridad) en la bandeja de tareas y realice las modificaciones en la pantalla de configuración.

- *Inicialización*
  - *Al utilizar Infineon TPM Professional Package, no es necesario inicializar TPM de antemano en Windows Vista®* **TPM Management on Local Computer** *(administración de TPM en el equipo local de Windows Vista).*
  - *Cuando TPM se inicializa en Infineon TPM Professional Package, no es necesario inicializar TPM en Windows Vista®* **TPM Management on Local Computer** *(administración de TPM en el equipo local de Windows Vista).*
- *Método de inicialización*

Al utilizar Professional Package V3.0 después de inicializar TPM mediante la función Windows Vista® **TPM Setting** *(configuración TPM de Windows Vista), se lleva a cabo la inicialización normal de la plataforma de la siguiente forma:*

1. *Tras instalar Professional Package V3.0, aparecerá "*`Initialized other OS`*" (inicializado otro sistema operativo) como mensaje del icono* **TPM** *de la barra de tareas.*

   ** Esto no significa que la TPM sea anormal.*

2. *Al ejecutar* **Infineon Security Platform Setting Tool** *(herramienta de configuración de la plataforma de seguridad Infineon) en el estado del Paso 1,* **[Security Platform State:]** (estado de la plataforma de seguridad), **[Owner:]** *(propietario) de la ficha* **Info** *(información) se mostrará como "*`Initialized (Failure Mode 2)`*" (inicializado - modo de fallo 2).*

   ** Esto no es un error. Sin embargo, la inicialización de la plataforma no habrá finalizado realmente.*

3. *Al ejecutar* **Security Platform User Initialization Wizard** *(asistente de inicialización de usuario de plataforma de seguridad), aparecerá una pantalla* **Initialization** *(inicialización). Aunque se haya seleccionado* **Security Platform restoration form a Backup Archive** *(restauración de plataforma de seguridad desde archivo de copia de seguridad), seleccione* **Security Platform Initialization** *(inicialización de la plataforma de seguridad).*

4. *En la siguiente pantalla de* **Initialize Security Platform** *(Inicializar plataforma de seguridad), introduzca la configuración de contraseña en Windows Vista®* **TPM Management on Local Computer** *(administración de TPM en el equipo local de Windows Vista). Durante este tiempo, no puede utilizar el* **TPM Owner Password Backup file** *(archivo de copia de seguridad de contraseña de propietario de TPM) guardado en* **TPM Management on Local Computer** *(administración de TPM en el equipo local).*

5. *Cuando Infineon TPM Professional Package cambia la contraseña de usuario, no se puede utilizar el* **TPM Owner Password Backup file** *(archivo de copia de seguridad de contraseña de propietario de TPM) creado en Windows Vista®* **TPM Management on Local Computer** *(administración de TPM en el equipo local de Windows Vista).*

3 Personal Secure Drive

La **Personal Secure Drive** (unidad segura personal) crea un almacén de datos para guardar información (archivos), lo que permite cifrar y guardar archivos de datos en la unidad virtual. Los archivos no simplemente se cifran y guardan en la unidad de disco duro. Dado que están protegidos por TPM, el nivel de seguridad es superior al que ofrece el cifrado basado en software ya existente. El tamaño mínimo de la PSD puede configurarse en 10 MB. El tamaño máximo de la PSD dependerá del sistema de archivos que cree la PSD. Consulte la ayuda para obtener más información.

3.1 Ventajas que ofrece Personal Secure Drive (unidad segura personal)

- Cifrado de la unidad virtual empleando la clave segura AES (Advanced Encryption Standard).
- Algoritmo RSA para generación de claves cifradas.
- Cifrado y descifrado automático de datos de seguridad transparente.
- Los archivos pueden protegerse fácilmente.
- Funcionamiento sencillo: Personal Secure Drive funciona de la misma forma que una unidad *Windows*® estándar.
- Procedimiento sencillo de administración y configuración mediante asistentes.

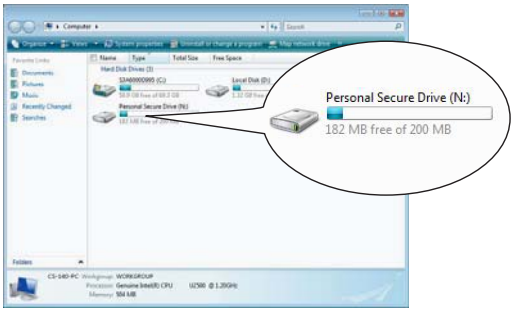
3.2 Personal Secure Drive (PSD): funcionamiento sencillo

1 Si se selecciona PSD en **Security Platform Features** (funciones de la plataforma de seguridad), haga clic en el icono **Security Platform** (plataforma de seguridad) de la bandeja de tareas tras iniciar una sesión en Windows y seleccione [**Personal Secure Drive**] - [**Load**] (cargar).

*Al hacer clic en el icono Security Platform (plataforma de seguridad) de la bandeja de tareas, podrá seleccionar [**Personal Secure Drive**] - [**Load**] (cargar), [**Unload**] (descargar) o [**Load at Logon**] (cargar al iniciar sesión).*

2 Aparecerá Infineon Security Platform User Authentication (autenticación de usuario de plataforma de seguridad de Infineon). Introduzca la contraseña de TPM. La unidad virtual PSD será reconocida una vez que se introduzca la contraseña correcta.

3 A continuación se ofrece una pantalla de ejemplo en la que se muestra la PSD detectada en el Explorador de *Windows*®.



En esta pantalla, aunque Personal Secure Drive se haya detectado como unidad **[N:]** con el nombre de unidad **Personal Secure Drive**, es posible cambiar esta configuración en **User Settings** (configuración de usuario) de **Infineon Security Platform Settings Tool** (herramienta de configuración de la plataforma de seguridad de Infeneon).

- *Dado que no se realiza una copia de seguridad de los archivos de la PSD mediante la función* **Backup** de **Infineon Security Platform Settings** *Tool, deberán emplearse métodos de copia de seguridad genéricos, como copiar los archivos de la PSD en un soporte externo extraíble en el explorador, para evitar pérdidas de datos.*
- *Los datos para el punto de restauración del sistema* establecidos por la función Restaurar sistema de Windows® se borran después de introducirse la contraseña de TPM durante el inicio de Windows, se monta la PSD y se asigna la unidad virtual. Es recomendable utilizar uno de los siguientes métodos para guardar los datos del punto de restauración del sistema.*
  - *No utilice la función PSD y utilice exclusivamente la función de cifrado de archivos a través de EFS.*
  - *Desactive temporalmente la función PSD justo antes de modificar el entorno Windows.*

  Desactive la función PSD -> Establezca el punto de restauración -> Modifique el sistema -> Compruebe que Windows se inicia correctamente -> Establezca el estado anterior de la función PSD.

  ** Consulte la Ayuda de Windows® para obtener detalles sobre el punto de restauración.*

- *La PSD debe establecerse para cada usuario de TPM. Por ejemplo, si hay dos usuarios de TPM registrados, A y B, B no podrá ver el contenido de la PSD de A.*
- *Dado que hay áreas de la PSD (Personal Secure Drive: unidad seguridad personal) que el sistema de archivos NTFS de Windows utiliza, la capacidad real de la PSD que puede utilizarse es inferior al valor inicial durante la configuración. Cuando se consume un mínimo de 10 MB y se aumenta la capacidad de la PSD, las áreas que utiliza NTFS también aumentan.*

  Cuando desee utilizar toda la capacidad requerida, deberá especificar una capacidad superior durante la configuración de la PSD.

  (ejemplo: Cuando desee utilizar alrededor de 200 MB, deberá especificar 220 MB como capacidad de la PSD durante la configuración.)

4 Secure E-Mail

En esta plataforma de seguridad, las ID digitales (Digital ID) utilizadas por el correo electrónico están protegidas por TPM, lo que las protege de pérdidas o robos.

Los programas de correo electrónico compatibles son Outlook®*, Windows Mail/Outlook Express* y Netscape®*.

* Tenga en cuenta que es posible que esta función no pueda utilizarse dependiendo de la versión del software.

4.1 Configuración

1 Adquiera una ID digital para su uso en Secure E-Mail (correo electrónico seguro) de Commercial Certificate Authority (CA). Consulte la ayuda de TPM para obtener detalles sobre CA.

2 Instale la Digital ID (ID digital) en el ordenador siguiendo los métodos de instalación y uso especificados por CA. Llegado este punto, asegúrese de que la ID digital está vinculada a TPM como Cryptographic Service Provider (CSP; proveedor de servicios criptográficos).

3 Establezca la configuración para Secure E-Mail en el software de correo electrónico. Consulte el manual de cada programa de correo electrónico y la ayuda de Infineon Security Platform para más detalles.

Establezca la configuración de **Secure E-mail** *(correo electrónico seguro) en Security Platform Features (funciones de plataforma de seguridad) al realizar el registro de usuario en TPM (paso 2.3) si no se ha asignado (*1, *2).*

*1 Uso de la Ayuda para consultar información relacionada con el correo electrónico y TPM

1) Haga doble clic en el icono **TPM** de la bandeja de tareas.
2) Seleccione la ficha **Info** (información).
3) Haga clic en el botón **Help** (Ayuda).
4) Realice búsquedas empleando palabras clave en la ficha **Search** (buscar) para localizar los temas sobre los que desee obtener más información. (Ejemplo: **E-Mail**)

*2 Activación de la función E-mail (correo electrónico) en User Settings (configuración de usuario)

1) Haga doble clic en el icono **TPM** de la bandeja de tareas.
2) Seleccione la ficha **User Settings** (configuración de usuario).
3) Haga clic en el botón **Configure** (configurar).
4) Active la opción **Secure E-mail** (correo electrónico seguro) y haga clic en el botón **Next** (siguiente).

5 EFS (Encrypting File System) Extension (extensión de EFS - sistema de cifrado de archivos-)

Si la opción File and Folder **encryption** (cifrado de archivos y carpetas) se activa en el paso 2.3, la función EFS del sistema operativo se amplía y el sistema se hace más seguro gracias a que la clave de cifrado del archivo cifrado por EFS queda protegida mediante TPM.

Las operaciones necesarias para cifrar/descifrar los archivos son muy similares.

La diferencia estriba en que al acceder inicialmente a los archivos cifrados mediante EFS después de iniciar una sesión en *Windows*®, es preciso introducir la contraseña de TPM del usuario que ha iniciado la sesión.

- *En el siguiente entorno, cuando los archivos creados en* **[Basic User Key and Other Folders]** *(clave básica de usuario y otras carpetas) se cifran mediante EFS, el software TPM no se inicia con normalidad y no será posible descifrar los datos cifrados.*
  - *TPM está instalada*
  - *La plataforma ha finalizado la inicialización*
  - *La función EFS se ha seleccionado durante la inicialización de usuario*

  Durante el estado de inicialización, los archivos de **[Basic User Key and Other Folders]** *(clave básica de usuario y otras carpetas) tienen atributos del sistema para evitar que se cifren. No cambie los atributos de archivo en las correspondientes carpetas.*

  ** En la configuración inicial de Windows, se ocultan las siguientes carpetas.*

  [Basic User Key and Other Folders] (clave básica de usuario y otras carpetas)

  ```
  C:\ProgramData\Infineon\TPM Software
  C:\ProgramData\Infineon\TPM Software 2.0
  C:\Users\All Users\Infineon
  ```

- *Si se cifran contenedores de archivos, copias de seguridad y archivos de fichas, éstos no se pueden descifrar en casos de emergencia.*

  Si se cifran la ficha de restablecimiento de contraseña y los archivos secretos, la contraseña no se puede restablecer.

  No cifre los siguientes archivos y carpetas.

  [Automatic Backup File] (archivo de copia de seguridad automática)

  Nombre de archivo predeterminado: SPSystemBackup.xml

  Contraseña predeterminada: No especificada (*)

  [Automatic Backup Data Storage Folder] (carpeta de almacenamiento de datos de copia de seguridad automática)

  Nombre de carpeta (fijo): SPSystemBackup (el archivo SPSystemBackup.xml se crea como subcarpeta de la carpeta que se está creando)

  [Emergency Recovery Token] (ficha de recuperación de emergencia)

  Nombre de archivo predeterminado: SPEmRecToken.xml

  Contraseña predeterminada: Soporte extraíble (disquete, memoria USB, etc.)

  [Password Reset Token] (ficha de restablecimiento de contraseña)

  Nombre de archivo predeterminado: SPPwdResetToken.xml

  Contraseña predeterminada: Soporte extraíble (disquete, memoria USB, etc.)

  [Basic User Password Reset] (restablecimiento de contraseña básica de usuario)

  Nombre de archivo predeterminado: SPPwdResetSecret.xml

  Contraseña predeterminada: Soporte extraíble (disquete, memoria USB, etc.)

  [Backup Archive] (archivo de copia de seguridad de PSD)

  Nombre de archivo predeterminado: SpBackupArchive.xml

  Contraseña predeterminada: No especificada (*)

  [PSD Backup Archive] (archivo de copia de seguridad de PSD)

  Nombre de archivo predeterminado: SpPSDBackup.fsb

  Paso predeterminado: No especificado (*)

  (*) Cuando se hace clic en **Reference** *(referencia), se abre "User folder\Documents\Security Platform".*

- *Al utilizar el cifrado de archivos mediante EFS, se recomienda que el usuario se familiarice con la información relativa a EFS contenida en la Ayuda de Windows®. Esto evitará que puedan descifrarse archivos debido al cambio accidental de la clave de cifrado utilizada en EFS o a la pérdida de la clave.*

6 Utilidad de contraseña de TOSHIBA

Empleando la Utilidad de contraseña de TOSHIBA, puede establecerse la configuración de forma que impida que los usuarios sin derechos de supervisor puedan cambiar la configuración relacionada con TPM en la configuración de la BIOS.

Una vez establecida esta configuración, los usuarios que no tengan derechos de supervisor no podrán cambiar la configuración relacionada con TPM en la configuración de la BIOS (elementos del cuadro **Security Controller** -controlador de seguridad-).

1. Ejecute el siguiente archivo para iniciar la Utilidad de contraseña de TOSHIBA.

   C:\Archivos de programa\TOSHIBA\PasswordUtility\TOSPU.exe

2. Registre la contraseña de supervisor en la ficha **Contraseña de supervisor**.
3. Abra la pantalla de configuración de la política de usuario desde la ficha **Contraseña de supervisor**.
4. En el cuadro **TPM**, desactive los elementos a los que no desea que puedan acceder o modificar los usuarios sin derechos de supervisor.
5. Pulse el botón **Definir** y, tras llevar a cabo la autenticación del supervisor, guarde la Política de usuario modificada.
6. Salga de la Utilidad de contraseña de TOSHIBA.

7 Migración del entorno TPM y eliminación

7.1 Migración

Haga clic en el icono **Security Platform** (plataforma de seguridad) en la barra de tareas y seleccione **Manage Security Platform** (administrar plataforma de seguridad). En la ventana **Infineon Security Platform Settings Tool** (herramienta de configuración de plataforma de seguridad Infineon), haga clic en la ficha **Migration** (migración). En la ficha **Migration**, al hacer clic en el botón **Learn more...** (más información) aparecen los detalles de la operación de migración. (La operación debe realizarse tanto para la plataforma de origen como para la plataforma de destino.) Realice la operación conforme a las instrucciones de la pantalla.

Sólo se migran los datos de TPM durante este proceso, de manera que realice la migración de datos dentro de la Personal Security Drive (unidad segura personal) y los archivos cifrados con EFS utilizando las operaciones de archivos habituales.

- *Recuerde que también es necesario instalar* **Infineon TPM Professional Package** *en la plataforma de destino.*
- *Si está activado Windows® Firewall, no es posible utilizar la migración entre los PC a través de la red. La configuración de Windows® Firewall puede cambiarse en* **Security Center** *(centro de seguridad) en el* **Panel de control***.*

7.2 Eliminación del PC

Al deshacerse del PC, realice los dos procesos siguientes para evitar la filtración de información confidencial. Haga lo mismo al cambiar el propietario del PC.

1 Desinstale **Infineon TPM Professional Package** y elimine el archivo de recuperación y la **Emergency Recovery Archive Token** (ficha de archivo de recuperación de emergencia). Elimine también todos los datos de la unidad de disco duro.

2 Paso 1: Muestre la pantalla **BIOS Setup** (configuración de la BIOS). (Consulte el Capítulo 2 - *Utilización de TPM por primera vez*.)

Paso 2: Mueva el cursor hasta la opción **Clear TPM Owner** (borrar propietario de TPM) en la configuración de **SECURITY CONTROLLER** (controlador de seguridad) y pulse la barra espaciadora o la tecla retroceso. Al hacer esto, se destruirán todos los datos contenidos en TPM y TPM quedará también desactivado a partir de ese momento.

Paso 3: Aparece un mensaje. Pulse las teclas **Y**, **E**, **S** seguidas de la tecla **Enter**.

Dado que se eliminan los datos de TPM, los archivos ya no podrán leerse.

8 Recuperación de TPM

8.1 Emergency Recovery Process (proceso de recuperación de emergencia): Descripción general

El proceso de recuperación de emergencia (Emergency Recovery Process) se utiliza:

- al cambiar el TPM debido a problemas de TPM.
- cuando la placa base con el TPM integrado presenta un defecto y se ha sustituido la placa base.
- cuando se ha borrado el TPM, bien sea accidentalmente o por cualquier otra razón.

Consulte *Restore Emergency Recovery Data Step by Step* (restaurar datos de recuperación de emergencia paso a paso) en la ayuda para más detalles.

- *Se recomienda imprimir antes una copia de la sección Restore Emergency Recovery Data Step by Step (restaurar datos de recuperación de emergencia paso a paso) de la ayuda.*
- *Las explicaciones que se ofrecen aquí son para la recuperación del contenido de TPM, no para la recuperación de datos relativos a TPM, como los archivos cifrados con EFS o los archivos de la PSD. Para los archivos de la unidad de disco duro integrada, se recomienda crear copias de seguridad independientes y almacenarlas de forma segura.*

8.2 Restablecimiento la contraseña de usuario

Esta función puede utilizarse en el caso de que el usuario de Infineon Security Platform (plataforma de seguridad Infineon) olvide la contraseña de usuario o si hay algún problema con el dispositivo de autenticación del usuario. Si la contraseña no se puede restablecer, el usuario no podrá utilizar las funciones de Security Platform. Esto podría dar como resultado la pérdida de datos secretos.

Consulte *Basic User Password Reset* (restablecimiento de contraseña de usuario básico) en la Ayuda para más detalles.

8.3 Restauración de PSD

Los datos de la PSD pueden recuperarse en el caso de que se pierda el certificado de PSD empleando Personal Secure Drive Recovery (recuperación de unidad segura personal).

Consulte *Personal Secure Drive Recovery* (recuperación de unidad segura personal) para más detalles.

Índice

A

Archivo de secreto personal 10
Automatic Backup
  archivo 18
  carpeta de almacenamiento de datos de copia de seguridad automática 18

B

Backup Archive (archivo de copia de seguridad) 18
Basic User Password
  pantalla 9
  restablecimiento 10, 18
BIOS
  configuración 6, 19
  pantalla 6
  pantalla de configuración 21

C

certificados 5
cifrado 5
Cifrado de sistema de archivos 17
cifrado secreto
  claves 5
  fórmulas 5
CLEAR OWNER 21
Commercial Certificate Authority (CA) 16
Configuración de la BIOS
  pantalla 6
Contraseña 5
  Emergency Recovery Token 8
  propietario 8
  usuario básico 9
Contraseña de supervisor 19
Contraseña de usuario
  restablecimiento 22
Copia de seguridad automática 8
Cryptographic Service Provider (CSP) 16

D

Digital ID 16

E

Emergency Recovery
  crear una nueva ficha 8
  ficha 8, 18
  ficha de archivo 21
  pantalla 8
  proceso 22

F

File and Folder encryption (EFS, cifrado de archivos y carpetas) 10

I

Infineon Security Platform
  herramienta de configuración 14
Infineon Security Platform Settings
  herramienta 14
Initialize Security Platform
  pantalla 12

M

Manage Security Platform (administrar plataforma de seguridad) 20
Maximum Basic User Password age (duración máxima de la contraseña de usuario básico) 11

P

Pantalla
copia de seguridad 8
inicialización 8
Password and Authentication 10
Security Platform Features 10, 11
User Initialization Wizard 9
Password Reset
crear una nueva ficha 9
ficha 9, 18
pantalla 9
Personal Secure Drive 11, 14
archivo de copia de seguridad de PSD 18
Política de usuario 19
pantalla de configuración 19
Propietario de TPM 9
punto de restauración 14

S

Secure E-mail 10, 16
Netscape 7, 10, 16
Outlook 7, 10, 16
Windows Mail/Outlook Express 10, 16
SECURITY CONTROLLER 6, 21
Security Platform
crear propietario 8
icono 8, 11, 20
icono Setting Tool 11
inicialización 8, 12
inicialización de usuario 11
pantalla Features 10, 11
restauración desde un archivo de copia de seguridad 12
User Initialization Wizard 12

T

TPM Management on Local Computer (administración de TPM en el equipo local) 12
TPM Owner Password Backup file (archivo de copia de seguridad de contraseña de propietario de TPM) 12

U

Utilidad de contraseña de TOSHIBA 19

W

Windows Firewall 20

Memorándum

Asegúrese de que las contraseñas empleadas se almacenan cuidadosamente (por si se olvidan) en un lugar al que no tengan acceso otras personas (para evitar la filtración de información secreta). No las almacene en lugares a los que puedan acceder personas no autorizadas (por ejemplo: pegadas a la superficie de una mesa).

Contraseña de propietario:

Contraseña de usuario básico:

Ubicación de almacenamiento de la ficha de recuperación de emergencia (Emergency Recovery Token):

Emergency Recovery Token Password (contraseña de ficha de recuperación de emergencia):

Ubicación de almacenamiento del archivo de copia de seguridad:

Ubicación de almacenamiento de la ficha de restablecimiento de contraseña (Password Reset Token):

Contraseña de ficha de restablecimiento de contraseña:

Ubicación de almacenamiento del archivo secreto personal:

Contraseña de usuario de TPM

Nombre de usuario de Windows®:

Contraseña de usuario de TPM:

Nombre de usuario de Windows®:

Contraseña de usuario de TPM:

Nombre de usuario de Windows®:

Contraseña de usuario de TPM: